Docket No. 1466.1023/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Seigo KOTANI et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: December 20, 2000

For: CRYPTOGRAPHIC COMMUNICATION METHOD, FILE ACCESS SYSTEM AND RECORDING MEDIUM

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. 2000-16657
Filed: January 26, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: December 20, 2000

By: _____

H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 １月２６日

出 願 番 号
Application Number: 特願２０００－０１６６５７

出 願 人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１０月 ６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

【書類名】　特許願

【整理番号】　9995327

【提出日】　平成12年 1月26日

【あて先】　特許庁長官殿

【国際特許分類】　H04K 1/00

【発明の名称】　暗号通信方法およびファイルアクセスシステム並びに記録媒体

【請求項の数】　14

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　東京都港区芝浦四丁目１５番３３号　株式会社富士通ビー・エス・シー内

【氏名】　佐々木　孝興

【発明者】

【住所又は居所】　東京都港区芝浦四丁目１５番３３号　株式会社富士通ビー・エス・シー内

【氏名】　山中　祐介

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　長谷部　高行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　秋山　良太

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100086933

【弁理士】

【氏名又は名称】　久保　幸雄

【電話番号】　06-6304-1590

【手数料の表示】

【予納台帳番号】　010995

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704487

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号通信方法およびファイルアクセスシステム並びに記録媒体

【特許請求の範囲】

【請求項１】

送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信方法であって、

送信側において、前記通信用の鍵とは異なる個別用の鍵で暗号化されたデータを送信するに当たり、前記暗号化されたデータを、前記個別用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵を用いて暗号化して送信する、

ことを特徴とする暗号通信方法。

【請求項２】

前記通信用の鍵を用いて暗号化する際に、元のデータのファイル識別子をファイル名に組み込み、暗号化されたデータであることを示す識別子を新たに付加する、

請求項１記載の暗号通信方法。

【請求項３】

送信側において鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、

受信側において、受信したデータを、前記通信用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵とは異なる個別用の鍵で暗号化して記憶するとともに、前記復号化されたデータを削除する、

ことを特徴とする暗号通信方法。

【請求項４】

前記個別用の鍵および前記通信用の鍵による暗号化または復号化を可能にするために、前記個別用の鍵および前記通信用の鍵に対してそれぞれ個別に認証を行う、

請求項１ないし請求項３のいずれかに記載の暗号通信方法。

【請求項５】

送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、

送信側において暗号化を行う際に、暗号化に用いた通信用の鍵に対応する識別コードを、暗号化されたデータに付加し、

受信側において、前記識別コードに対応した通信用の鍵を用いて復号化する、

ことを特徴とする暗号通信方法。

【請求項６】

送信側において通信用の鍵を複数個準備しておき、それらのうちの１つの鍵を用いてデータを暗号化するとともに、暗号化に用いた鍵に対応する識別コードを暗号化されたデータに付加する、

請求項５記載の暗号通信方法。

【請求項７】

受信側において通信用の鍵を複数個準備しておき、それらのうちの前記識別コードに対応した通信用の鍵を選択して用いる、

請求項５記載の暗号通信方法。

【請求項８】

互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とし、

１つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う、

ことを特徴とするファイルアクセスシステム。

【請求項９】

互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とし、

処理対象のファイルが暗号化されているか否かを判別し、暗号化されている場合に一方の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、

続いて、暗号化されていないファイルを他方の鍵を用いて暗号化する、

ことを特徴とするファイルアクセスシステム。

【請求項１０】

互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とし、

暗号化されているファイルを一方の鍵を用いて復号化し、

ファイルの格納先が暗号化ファイル用であるか否かを判別し、暗号化ファイル用である場合に前記ファイルを他方の鍵で暗号化して格納し、暗号化ファイル用でない場合に前記ファイルをそのまま格納する、

ことを特徴とするファイルアクセスシステム。

【請求項１１】

第１のホルダおよび第２のホルダを示す画面を表示し、

前記第１のホルダに格納されたファイルを前記第２のホルダに移動する指示入力があったときに、前記第１のホルダに格納されたファイルの復号化および／または暗号化を行い、復号化および／または暗号化されたファイルを前記第２のホルダに格納する、

ことを特徴とするファイルアクセスシステム。

【請求項１２】

前記第１のホルダに格納されたファイルが暗号化されているか否かを判別し、暗号化されている場合に第１の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、

続いて、暗号化されていないファイルを第２の鍵を用いて暗号化する、

請求項１１記載のファイルアクセスシステム。

【請求項１３】

ファイルへのアクセスのためのプログラムを記録した記録媒体であって、

互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とする処理と、

１つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う処理と、

をコンピュータに実行させるためのプログラムを格納したコンピュータ読み取り可能な記録媒体。

【請求項１４】

送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信に用いられる暗号化処理装置であって、

前記通信用の鍵と、

前記通信用の鍵とは異なる個別用の鍵と、

前記個別用の鍵による復号化および前記通信用の鍵による暗号化を連続的に行う処理部とを有してなる、

ことを特徴とする暗号化処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号通信方法およびファイルアクセスシステム並びに記録媒体に関する。

【０００２】

パーソナルコンピュータが普及し、パソコン通信または電子メールなどのネットワークを介した通信が業務上欠かせないものとなっている。個別のパーソナルコンピュータで用いるデータのみでなく、それらのデータをネットワークを介して通信することをも考慮して、データのセキュリティの保護を総合的に図る必要がある。

【０００３】

【従来の技術】

従来において、電子メールなどで通信を行うデータのセキュリティの保護のために、鍵を用いてデータを暗号化して送信し、受信側において受信したデータを送信側と共通の鍵を用いて復号化する通信方法が知られている。

【０００４】

一方、パーソナルコンピュータで扱うファイルのセキュリティの保護のためのファイルアクセスシステムを、本出願人は特開平１０－３０１８５６号として提案した。これによると、認証により使用権限が確認されて鍵が活性化されている間において、任意のファイルを指定のホルダに入れるとそれが自動的に暗号化され、且つそのホルダ内のファイルを読み出す際には自動的に復号化される。使用権限を有するユーザは、暗号化されたファイルを通常のファイルと同じように閲覧し編集することができ、ファイルが暗号化されていることを全く意識する必要

がない。

【０００５】

【発明が解決しようとする課題】

上に述べたファイルアクセスシステムは、個人用のコンピュータの内部において、データベースまたはファイルなどの種々のコンテンツ類を扱うのに非常に優れたシステムである。

【０００６】

しかしながら、自分のコンテンツを暗号化して他者に送信したい場合、または他者から送信された暗号化コンテンツを個人用の鍵で暗号化して運用したい場合などにおいて、そのままでは不都合が生じる。

【０００７】

つまり、例えば、暗号化されたコンテンツを電子メールの添付ファイルとして送信する場合に、添付ファイルとするためのリード命令によって添付ファイルが自動的に復号化されてしまう。これを防ぐには、鍵の機能を事前に停止させる必要があるが、そのための操作が煩雑であるので、暗号化されていない添付ファイルを誤って送信してしまうおそれがある。

【０００８】

また、暗号化されていないコンテンツを暗号化した添付ファイルとして送信する場合に、鍵を活性化して一旦暗号化を行い、その後に鍵の機能を停止させた上で、リード命令によって添付ファイルとする必要がある。この場合も操作が煩雑であり、操作を誤って復号化された添付ファイルを送信してしまう可能性がある。

【０００９】

本発明は、上述の問題に鑑みてなされたもので、暗号化されたデータおよび暗号化されていないデータを混在して扱う場合などにおいて、容易な操作で間違うことなく暗号通信を行えるようにすることを目的とする。

【００１０】

【課題を解決するための手段】

請求項１の発明に係る方法は、送信側において通信用の鍵を用いてデータを暗

号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信方法であって、送信側において、前記通信用の鍵とは異なる個別用の鍵で暗号化されたデータを送信するに当たり、前記暗号化されたデータを、前記個別用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵を用いて暗号化して送信する。

【００１１】

請求項２の発明に係る方法では、前記通信用の鍵を用いて暗号化する際に、元のデータのファイル識別子をファイル名に組み込み、暗号化されたデータであることを示す識別子を新たに付加する。

【００１２】

請求項３の発明に係る方法は、送信側において鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、受信側において、受信したデータを、前記通信用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵とは異なる個別用の鍵で暗号化して記憶するとともに、前記復号化されたデータを削除する。

【００１３】

請求項４の発明に係る方法では、前記個別用の鍵および前記通信用の鍵による暗号化または復号化を可能にするために、前記個別用の鍵および前記通信用の鍵に対してそれぞれ個別に認証を行う。

【００１４】

請求項５の発明に係る方法は、送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、送信側において暗号化を行う際に、暗号化に用いた通信用の鍵に対応する識別コードを、暗号化されたデータに付加し、受信側において、前記識別コードに対応した通信用の鍵を用いて復号化する。

【００１５】

請求項６の発明に係る方法では、送信側において通信用の鍵を複数個準備しておき、それらのうちの１つの鍵を用いてデータを暗号化するとともに、暗号化に用いた鍵に対応する識別コードを暗号化されたデータに付加する。

【００１６】

請求項７の発明に係る方法では、受信側において通信用の鍵を複数個準備しておき、それらのうちの前記識別コードに対応した通信用の鍵を選択して用いる。

請求項８の発明に係るシステムは、互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とし、１つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う。

【００１７】

請求項９の発明に係るシステムは、互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とし、処理対象のファイルが暗号化されているか否かを判別し、暗号化されている場合に一方の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、続いて、暗号化されていないファイルを他方の鍵を用いて暗号化する。

【００１８】

請求項１０の発明に係るシステムは、互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とし、暗号化されているファイルを一方の鍵を用いて復号化し、ファイルの格納先が暗号化ファイル用であるか否かを判別し、暗号化ファイル用である場合に前記ファイルを他方の鍵で暗号化して格納し、暗号化ファイル用でない場合に前記ファイルをそのまま格納する。

【００１９】

請求項１１の発明に係るシステムは、第１のホルダおよび第２のホルダを示す画面を表示し、前記第１のホルダに格納されたファイルを前記第２のホルダに移動する指示入力があったときに、前記第１のホルダに格納されたファイルの復号化および／または暗号化を行い、復号化および／または暗号化されたファイルを前記第２のホルダに格納する。

【００２０】

請求項１２の発明に係るシステムは、前記第１のホルダに格納されたファイルが暗号化されているか否かを判別し、暗号化されている場合に第１の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、続いて、暗号化されていないファイルを第２の鍵を用いて暗号化する。

【００２１】

請求項１３の発明に係る記録媒体は、ファイルへのアクセスのためのプログラムを記録した記録媒体であって、互いに異なる２つの鍵をそれぞれ個別に認証することによって使用可能とする処理と、１つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う処理と、をコンピュータに実行させるためのプログラムを格納したコンピュータ読み取り可能な記録媒体でである。

【００２２】

請求項１４の発明に係る装置は、送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信に用いられる暗号化処理装置であって、前記通信用の鍵と、前記通信用の鍵とは異なる個別用の鍵と、前記個別用の鍵による復号化および前記通信用の鍵による暗号化を連続的に行う処理部とを有してなる。

【００２３】

本発明において、送信側において用いられる通信用の鍵と、受信側において用いられる通信用の鍵とは、共通の同じ鍵であってもよいし、また、互いに異なる別の鍵であってもよい。

【００２４】

【発明の実施の形態】

図１は通信システム１の例を示すブロック図、図２は暗号化カードＳＰＣの構成を示すブロック図、図３はグループ鍵による暗号化処理を行う前後のファイルの状態を示す図である。

【００２５】

図１において、通信システム１は、ネットワークＮＷに接続された複数の通信端末５ａ，５ｂ，…からなる。ネットワークＮＷは、ＬＡＮ、ＷＡＮ、公衆回線、専用回線、無線回線、またはインターネットなど、若しくはそれらの組み合わせによるネットワークである。また、複数のネットワークを介したネットワークＮＷであってもよい。通信端末５ａ，５ｂ，…として、例えばパーソナルコンピュータを用いることができ、その構成の一例が図に示されている。以降において

、通信端末５ａ，５ｂ，…のいずれかかまたは全体を指して「通信端末５」と記載することがある。

【００２６】

通信端末５は、処理装置１１、表示装置１２、ドライブ装置１３、入力装置１４、暗号化カードＳＰＣ、その他の装置から構成される。

処理装置１１は、ＣＰＵ、ＲＯＭ、主メモリ、外部記憶装置、通信制御回路、種々のインタフェース、その他の周辺回路などを備え、他の装置、特に暗号化カードＳＰＣとも協働して本発明に係る暗号通信のための処理、ファイルアクセス処理、その他の種々の処理を行う。外部記憶装置には、本発明に係る暗号通信のためのアプリケーションプログラム、他のプログラム、種々のファイル、テーブル、データベース、その他のデータが記憶される。

【００２７】

表示装置１２は、その表示面ＨＧに、画像、文字、および後述する種々の画面を表示する。

ドライブ装置１３は、ＣＤ－ＲＯＭ（ＣＤ）、フロッピーディスクＦＤ、または光磁気ディスクなどの記録媒体がセットされたときに、それにアクセスしてデータまたはプログラムの読み書きを行う。

【００２８】

入力装置１４は、キーボード、マウス、または他のポインティングデバイスなどであり、データを入力しまたは処理装置１１に指令を与えるために用いられる。

【００２９】

図２に示すように、暗号化カードＳＰＣは、暗号化処理部２１、復号化処理部２２、および鍵部３２を備える。

鍵部３２には、多数の鍵Ｋ１，Ｋ２，Ｋ３…が格納されている。図では１２個の鍵Ｋが示されているが、それ以下であってもよく、またそれ以上、例えば１６個であってもよい。これらの各鍵Ｋは、それぞれの識別コードと対応付けられている。暗号化カードＳＰＣを使用する際には、その起動時に使用権限を確認するための認証が行われるが、その際に入力されるユーザＩＤまたはグループＩＤが

その識別コードに対応し、それと一致する鍵Ｋが選択されるようになっている。ユーザＩＤ（個別ＩＤ）により選択される鍵Ｋは個別鍵ＫＰとして機能し、グループＩＤにより選択される鍵Ｋはグループ鍵ＫＧとして機能する。

【００３０】

なお、この例の実施形態においては、暗号通信を行う場合に、送信側および受信側において、少なくとも１つの共通の鍵Ｋを持っておく必要がある。

暗号化処理部２１および復号化処理部２２は、鍵部３２から選択された鍵Ｋを用いて、暗号化処理または復号化処理を行う。これらの処理は可逆処理である。つまり、暗号化処理を行った後に復号化処理を行うことにより、またその逆を行うことにより、元の状態に戻る。このときの処理の例の詳細は、上に述べた特開平１０－３０１８５６号を参照することができる。

【００３１】

但し、グループ鍵ＫＧによる暗号化処理または復号化処理を行う場合には、元のデータに対して、ヘッダを付加しまたは削除する処理が行われる。

すなわち、例えば、図３（Ａ）に示すように、ヘッダＨＤ、本文ＢＤ、フッタＦＯ、からなる１つのファイルＦＬ１があった場合に、グループ鍵ＫＧを用いてこれの暗号化処理を行うと、図３（Ｂ）に示すように、ファイルＦＬ１の全体が暗号化されて本文ＣＢＤとなり、これに新たなヘッダＣＨＤが付加されたファイルＦＬ２となる。その際に、グループ鍵ＫＧに対応する識別コード（グループＩＤ）が属性情報としてヘッダＣＨＤに付加される。グループ鍵ＫＧを用いてファイルＦＬ２の復号化処理を行うと、ファイルＦＬ１に戻る。

【００３２】

なお、暗号化カードＳＰＣは、本実施形態においてはＰＣカードの形態で用いられるが、他の形態であってもよい。また、本実施形態においては暗号化カードＳＰＣによって暗号化処理および復号化処理を行っているが、暗号化カードＳＰＣを用いることなく、同様の処理をソフトウエアによって実行することも可能である。

【００３３】

図４は通信端末５ａ，５ｂの暗号通信時における機能を示すブロック図である

。なお、図４においては、通信端末５ａを送信側とし、通信端末５ｂを受信側としてあるが、各通信端末５によって送信および受信のいずれをも行うことができる。

【００３４】

図４において、送信側の通信端末５ａは、暗号ホルダＦＡ、平文ホルダＦＨ、送受信ホルダＦＴ、および暗号化カードＳＰＣを有する。

暗号ホルダＦＡは、それが活性化されているときに、他のホルダから暗号ホルダＦＡにファイルを移動した際に、自動的にそのファイルの暗号化処理が行われ、暗号化されたファイル（暗号ファイル）として暗号ホルダＦＡに格納される。また、暗号ホルダＦＡに格納されているファイル（暗号ファイル）を、暗号ホルダＦＡから他のホルダに移動した際には、自動的にそのファイルの復号化処理が行われ、復号化されたファイル（平文ファイル）として移動先のホルダに格納される。

【００３５】

つまり、暗号ホルダＦＡに入ってくる際には暗号化処理が行われ、暗号ホルダＦＡから出ていく際には復号化処理が行われる。この際に、移動するファイルの種類は問わない。例えばそれが暗号ファイルであっても平文ファイルであってもよい。例えば、もし暗号ファイルが暗号ホルダＦＡに入ってくると、再度の暗号化処理が行われ、これは復号化処理を２回行うことによって平文ファイルに戻すことができる。

【００３６】

そして、暗号ホルダＦＡに格納された暗号ファイルは、それを読み出す際には自動的に復号化され、平文ファイルが表示面ＨＧに表示されまたはプリンタで印刷される。したがって、ユーザは、暗号ホルダＦＡ内の暗号ファイルを通常のファイルと同じように閲覧し編集することができ、ファイルが暗号化されていることを全く意識する必要がない。

【００３７】

暗号ホルダＦＡへの入出時のファイルの暗号化処理または復号化処理に用いられる鍵Ｋは、個別鍵ＫＰが用いられる。

平文ホルダＦＨは、一般的なＯＳまたはアプリケーションの下で作成される通常の任意のホルダである。平文ホルダＦＨには、暗号化されていない平文ファイルが格納される。但し、暗号ファイルをも格納することはできる。

【００３８】

図４に破線で示すように、平文ホルダＦＨ内の平文ファイルを暗号ホルダＦＡ内に移動させると、個別鍵ＫＰによる暗号化処理が行われ、暗号ホルダＦＡには暗号ファイルが格納される。

【００３９】

送受信ホルダＦＴは、暗号通信に用いる送信用のファイルおよび受信した受信ファイルを格納するホルダである。一般のＯＳまたはアプリケーションで提供されるホルダのうちのどれを送受信ホルダＦＴに設定するかは、後で述べるようにユーザが選択することができる。送受信ホルダＦＴに格納したファイルを送信するには、例えばそのファイルを電子メールの添付ファイルとすればよい。また、電子メールで受信したファイルが、この送受信ホルダＦＴに入るように設定すればよい。

【００４０】

暗号ホルダＦＡに格納された暗号ファイルを送受信ホルダＦＴに移動する際に、まず個別鍵ＫＰを用いて復号化処理２２が行われ、続いて、復号化されたファイルに対し、グループ鍵ＫＧを用いて暗号化処理２１が行われる。つまり、個別鍵ＫＰで暗号化されて暗号ホルダＦＡに格納されていた暗号ファイルは、グループ鍵ＫＧで暗号化された暗号ファイルとして送受信ホルダＦＴに格納される。なお、図には示されないが、復号化処理２２および暗号化処理２１のために、一時的なホルダが設けられる。

【００４１】

また、平文ホルダＦＨに格納された平文ファイルを送受信ホルダＦＴに移動した際には、グループ鍵ＫＧを用いて暗号化処理２１が行われる。つまり、個別鍵ＫＰで暗号化されて暗号ホルダＦＡに格納されていた暗号ファイルは、グループ鍵ＫＧで暗号化された暗号ファイルとして送受信ホルダＦＴに格納される。

【００４２】

このように、暗号ホルダＦＡまたは平文ホルダＦＨのいずれに格納されていたファイルであっても、暗号化カードＳＰＣを通過することにより、グループ鍵ＫＧで暗号化された暗号ファイルが送受信ホルダＦＴに格納されることになる。したがって、暗号ファイルまたは平文ファイルのいずれであっても、それを電子メールの添付ファイルとする場合に、容易にグループ鍵ＫＧで暗号化された暗号ファイルとすることができる。

【００４３】

次に、受信側の通信端末５ｂは、暗号ホルダＦＡ、平文ホルダＦＨ、送受信ホルダＦＴ、および暗号化カードＳＰＣを有する。

暗号ホルダＦＡ、平文ホルダＦＨ、および送受信ホルダＦＴは、上にのべたと同様である。

【００４４】

受信した電子メールまたはその添付ファイルが送受信ホルダＦＴに入ったとする。つまり、送受信ホルダＦＴには、グループ鍵ＫＧで暗号化された暗号ファイルが格納される。

【００４５】

送受信ホルダＦＴに格納された暗号ファイルを暗号ホルダＦＡに移動した際に、まずグループ鍵ＫＧを用いて復号化処理２２が行われ、続いて、復号化されたファイルに対し、個別鍵ＫＰを用いて暗号化処理２１が行われる。つまり、グループ鍵ＫＧで暗号化されて送信され送受信ホルダＦＴに格納されていた暗号ファイルは、個別鍵ＫＰで暗号化された暗号ファイルとして暗号ホルダＦＡに格納される。

【００４６】

また、送受信ホルダＦＴから平文ホルダＦＨに移動した際には、グループ鍵ＫＧを用いて復号化処理２２が行われる。つまり、送受信ホルダＦＴに格納されていた暗号ファイルは、グループ鍵ＫＧで復号化された平文ファイルとして平文ホルダＦＨに格納される。

【００４７】

このように、送受信ホルダＦＴに格納された暗号ファイルは、暗号化カードＳ

ＰＣを通過することにより、個別鍵ＫＰで暗号化された暗号ファイルとして暗号ホルダＦＡに格納され、または平文ファイルとして平文ホルダＦＨに格納されることとなる。

【００４８】

なお、各通信端末５において、暗号化カードＳＰＣの使用に先立って、ユーザＩＤおよびグループＩＤを入力して個別鍵ＫＰおよびグループ鍵ＫＧを選択し、それらを活性化しておく必要がある。

【００４９】

次に、通信端末５における処理をフローチャートおよび画面を参照してさらに詳しく説明する。

図５は個別セキュリティの処理を示すフローチャート、図６は通信セキュリティの処理を示すフローチャート、図７は暗号送信処理を示すフローチャート、図８は暗号受信処理を示すフローチャート、図９はグループ鍵での復号化処理を示すフローチャート、図１０は個別ＩＤ認証画面ＨＧ１を示す図、図１１は個別鍵ＫＰが活性化された状態の画面ＨＧ２を示す図、図１２は暗号通信のためのプルダウンメニュの画面ＨＧ３を示す図、図１３はグループＩＤ認証画面ＨＧ４を示す図、図１４は送信時における送信ファイルの選択の状態を示す図、図１５は受信時における受信ファイルの状態を示す図である。

【００５０】

図５に示す個別セキュリティは、通信を行うことなく、通信端末５の内部において個別鍵ＫＰのみを用いてファイルのセキュリティを確保するために必要な前処理である。

【００５１】

すなわち、暗号通信のためのアプリケーション（または個別セキュリティのためのアプリケーション）を立ち上げると、まず最初に図１０に示す個別ＩＤ認証画面ＨＧ１が表示されるので、個別ＩＤ（ユーザＩＤ）およびパスワードを入力し、「ＯＫ」ボタンを押す（クリックする）（＃１１）。

【００５２】

そうすると、入力された個別ＩＤおよびパスワードの認証が行われる（＃１２

）。認証がＯＫであれば、その個別ＩＤに対応する個別鍵ＫＰが有効となる（＃１３）。したがって、同じ通信端末５であっても、ユーザ毎に個別ＩＤおよびパスワードを設定しておくことによって、複数のユーザがそれぞれのセキュリティを確保することができる。

【００５３】

図１１に示すように、個別鍵ＫＰが有効となったことを示す鍵マークを示す画面ＨＧ２が表示され（＃１４）、暗号ホルダＦＡが活性化される（＃１５）。

図６に示す通信セキュリティは、暗号通信を行うに必要な前処理である。

【００５４】

図１１に示す画面ＨＧ２の鍵マークを右クリックすると、図１２に示すように、暗号通信のためのプルダウンメニュを示す画面ＨＧ３が表示される。ここで「暗号通信」をクリックすると、図１３に示すグループＩＤ認証画面ＨＧ４が表示される。そこで、グループＩＤおよびパスワードを入力し、「ＯＫ」ボタンを押す（＃２１）。

【００５５】

そうすると、入力されたグループＩＤおよびパスワードの認証が行われる（＃２２）。認証がＯＫであれば、そのグループＩＤに対応するグループ鍵ＫＧが有効となる（＃２３）。これとともに、次の画面ＨＧ５～８が表示される。

【００５６】

なお、グループＩＤを入力する際に、送信先に応じたグループＩＤを入力するようにすればよい。つまり、複数の送信先を予め設定しておき、且つ送信先に応じて異なるグループＩＤを割り当てておく。そして、各送信先においても、同じグループＩＤを用いることに決めておく。これによって、通信の予定された２つまたは３つ以上の通信端末５間において、且つそれらの通信端末５間においてのみ、同じグループＩＤつまり同じグループ鍵ＫＧが用いられることとなり、セキュリティの維持が確実となる。

【００５７】

図６において、送信する場合には（＃２４でイエス）、暗号送信処理が行われ（＃２５）、受信する場合には（＃２６でイエス）、暗号受信処理が行われ（＃

２７）。

【００５８】

図７において、暗号送信処理では、まず、送信ファイルの選択が行われる（＃３１）。

すなわち、図１４（Ａ）に示す画面ＨＧ５において、左側に運用ホルダＦＵが、右側に送受信ホルダＦＴが表示され、それぞれの上に参照ボタンＢＴ３，４が表示され、中央にそれらの間の変換を指示する変換ボタンＢＴ１，２が表示される。

【００５９】

参照ボタンＢＴ３を押すと、ホルダのリストが表示されるので、その中から運用ホルダＦＵとして設定するホルダを選択する。

参照ボタンＢＴ４を押すと、ホルダのリストが表示されるので、その中から送受信ホルダＦＴとして設定するホルダを選択する。

【００６０】

図１４（Ｂ）に示す状態では、運用ホルダＦＵには「○×．ｄｏｃ」および「△□．ｄｏｃ」の２つのファイル（平文ファイル）が格納されている。ここで、変換ボタンＢＴ１を押すと、図１４（Ｃ）に示すように、それらのファイルに対する暗号化処理が行われるとともに、ファイルは運用ホルダＦＵから送受信ホルダＦＴに移動し、運用ホルダＦＵ内にあったファイルは削除される。

【００６１】

すなわち、図７において、運用ホルダＦＵのファイルが暗号ファイルであった場合には（＃３２でイエス）、個別鍵ＫＰで復号化し（＃３３）、続いてグループ鍵ＫＧで暗号化する（＃３４）。運用ホルダＦＵのファイルが暗号ファイルでなかった場合には（＃３２でノー）、そのままグループ鍵ＫＧで暗号化する（＃３４）。

【００６２】

グループ鍵ＫＧによる暗号化の際に、元のファイルのファイル識別子がファイル名に組み込まれ、暗号化されたファイルであることを示す識別子が新たに付加される。また、グループ鍵ＫＧに対応するグループＩＤが、属性情報としてヘッ

ダに書き込まれる。

【００６３】

図１４（Ｂ）（Ｃ）に示す例では、ファイル名「○×．ｄｏｃ」がファイル名「○×ｄｏｃ．ｅｎｃ」と変更されている。つまり、元のファイルのファイル識別子「ｄｏｃ」がファイル名に組み込まれて「○×ｄｏｃ」となり、暗号化されたファイルであることを示す識別子「ｅｎｃ」が新たに付加されている。

【００６４】

なお、暗号化されたファイルであることを示す識別子に、グループＩＤを示す符号を付加しておくことも可能である。

図８において、暗号受信処理では、まず、受信ファイルの選択が行われる（＃４１）。

【００６５】

すなわち、図１５に示す画面ＨＧ８において、参照ボタンＢＴ４を押すと、ホルダのリストが表示されるので、その中から送受信ホルダＦＴとして設定するホルダを選択する。

【００６６】

参照ボタンＢＴ３を押すと、ホルダのリストが表示されるので、その中から運用ホルダＦＵとして設定するホルダを選択する。

図１５に示す状態では、送受信ホルダＦＴには「○×ｄｏｃ．ｅｎｃ」および「△□ｄｏｃ．ｅｎｃ」の２つのファイルが格納されている。ここで、変換ボタンＢＴ２を押すと、それらのファイルに対する復号化処理が行われるとともに、ファイルは送受信ホルダＦＴから運用ホルダＦＵに移動し、送受信ホルダＦＴ内にあったファイルは削除される。

【００６７】

すなわち、図８において、送受信ホルダＦＴ内のファイルがグループ鍵ＫＧで復号化される（＃４２）。格納先のホルダ（運用ホルダＦＵ）が暗号ホルダＦＡであった場合には（＃４３でイエス）、さらに個別鍵ＫＰで暗号化され（＃４４）、その後、平文ファイルが削除される（＃４５）。

【００６８】

なお、復号化を行った後で受信したファイル自体を自動的に削除するか否かについて、ユーザが設定することができる。また、図１５に示す送受信ホルダＦＴに、識別子が「ｅｎｃ」でないファイルが格納された場合には、その旨の警報が表示される。

【００６９】

図９において、グループ鍵ＫＧでの復号化処理では、対象となるファイルのヘッダのグループＩＤが抽出される（＃５１）。そして、抽出されたグループＩＤと、予め認証のために入力されたグループＩＤとが比較され、認証済のグループ鍵ＫＧが正しいか否かが判断される（＃５２）。合っていない場合に、グループＩＤの再入力などを行う（＃５３）。

【００７０】

そして、ヘッダを除去し（＃５４）、グループ鍵ＫＧを復号化を行い（＃５５）、ファイル名を復元する（＃５６）。

なお、受信側において、使用可能なグループ鍵ＫＧが複数個ある場合に、受信したファイルのヘッダから抽出されたグループＩＤによって使用するグループ鍵ＫＧを自動的に選択するようにしてもよい。このようにすると、グループ鍵ＫＧの異なる複数の送信側から送られた暗号ファイルを受信した際に、受信側においてそれぞれのグループ鍵ＫＧを自動的に選択して復号化を行うことが可能となる。

【００７１】

次に、暗号通信のための操作方法の異なる他の実施形態について説明する。

図１６は他の実施形態を示す送信ファイルの選択処理のフローチャート、図１７はファイル選択のメイン画面ＨＧ２１を示す図である。

【００７２】

個別セキュリティのためのアプリケーションが立ち上がった状態で、つまり個別ＩＤの認証が終了している状態で、暗号通信のためのアプリケーションを立ち上げると、まず最初に図１７に示すメイン画面ＨＧ２１が表示される。

【００７３】

メイン画面ＨＧ２１では、ファイル選択ボタンＢＴ２１、暗号化ボタンＢＴ２

２、復号化ボタンＢＴ２３、オプションボタンＢＴ２４、リスト表示欄ＦＣ、および図示しないプログレスバーが表示される。

【００７４】

ファイル選択ボタンＢＴ２１を押すと、Windows 標準のファイル選択画面が表示されるので、その中から暗号化または復号化の対象となるファイルを選択する。選択したファイル名がリスト表示欄ＦＣに表示される（＃１０１）。

【００７５】

暗号化ボタンＢＴ２２を押すと、図１３に示すグループＩＤ認証画面ＨＧ４が表示されるので、グループＩＤおよびパスワードを入力し、「ＯＫ」ボタンを押す（＃１０２）。入力されたグループＩＤおよびパスワードの認証が行われ（＃１０３）、認証がＯＫであれば、そのグループＩＤに対応するグループ鍵ＫＧが有効となる（＃１０４）。

【００７６】

これとともに、暗号ファイルの格納先を選択する画面が表示されるので、適当な格納先を指定する（＃１０５）。対象となるファイルが暗号ファイルであった場合には（＃１０６でイエス）、個別鍵ＫＰで復号化した後（＃１０７）、グループ鍵ＫＧで暗号化を行う（＃１０８）。暗号ファイルでない場合には、そのままグループ鍵ＫＧで暗号化を行う（＃１０８）。

【００７７】

上に述べた通信システム１によると、暗号化されたファイルおよび暗号化されていないファイルが混在している場合でも、容易な操作で間違うことなく暗号通信を行うことができる。

【００７８】

上の実施形態において、通信端末５として、パームトップ型、ノート型、ラップトップ型、デスクトップ型、その他の種々の形式のパーソナルコンピュータまたは情報端末を用いることができる。

【００７９】

上の実施形態においては、送信側および受信側において、少なくとも１つの共通のグループ鍵ＫＧを準備しておくいわば共通鍵暗号方式の場合を説明したが、

送信側と受信側とで共通の鍵Ｋを準備することなく、互いに異なる鍵を用いて暗号化と復号化とを行うようにしてもよい。また、例えば、公開鍵暗号方式を採用する場合には、暗号化を行う鍵を公開し、復号化を行う鍵のみを秘密にしておけばよい。その他、通信システム１の全体または各部の構成、処理の内容、順序、および画面の構成などは、本発明の趣旨に沿って適宜変更することができる。

【００８０】

【発明の効果】

本発明によると、暗号化されたファイルおよび暗号化されていないファイルを混在して扱う場合などにおいても、容易な操作で間違うことなく暗号通信を行うことができる。

【図面の簡単な説明】

【図１】

通信システムの例を示すブロック図である。

【図２】

暗号化カードの構成を示すブロック図である。

【図３】

グループ鍵により暗号化処理を行った際のファイルの状態の変化を示す図である。

【図４】

通信端末の暗号通信時における機能を示すブロック図である。

【図５】

個別セキュリティの処理を示すフローチャートである。

【図６】

通信セキュリティの処理を示すフローチャートである。

【図７】

暗号送信処理を示すフローチャートである。

【図８】

暗号受信処理を示すフローチャートである。

【図９】

グループ鍵での復号化処理を示すフローチャートである。

【図１０】

個別ＩＤ認証画面を示す図である。

【図１１】

個別鍵が活性化された状態を示す画面である。

【図１２】

暗号通信のためのプルダウンメニュを示す画面である。

【図１３】

グループＩＤ認証画面を示す図である。

【図１４】

送信時における送信ファイルの選択の状態を示す図である。

【図１５】

受信時における受信ファイルの状態を示す図である。

【図１６】

他の実施形態を示す送信ファイルの選択処理のフローチャートである。

【図１７】

ファイル選択のメイン画面を示す図である。

【符号の説明】

１　通信システム

５　通信端末（ファイルアクセスシステム）

１１　処理装置

ＳＰＣ　暗号化カード（暗号化処理装置）

Ｋ　鍵

ＫＰ　個別鍵（個別用の鍵、一方の鍵、第１の鍵）

ＫＧ　グループ鍵（通信用の鍵、他方の鍵、第２の鍵）

ＦＵ　運用ホルダ（第１のホルダ）

ＦＴ　送受信ホルダ（第２のホルダ）

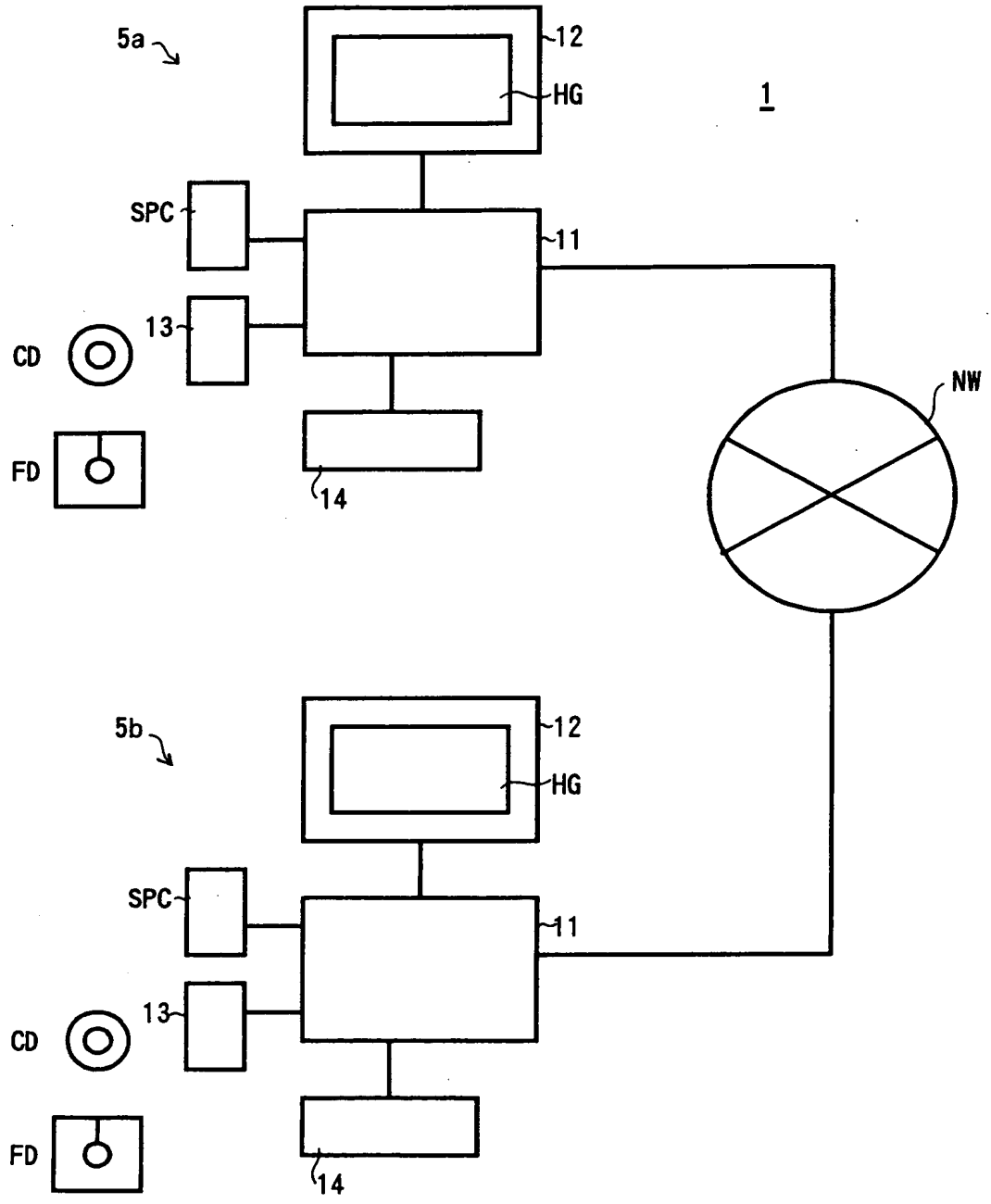
ＣＤ　ＣＤ－ＲＯＭ（記録媒体）

ＦＤ　フロッピーディスク（記録媒体）

【書類名】　　図面

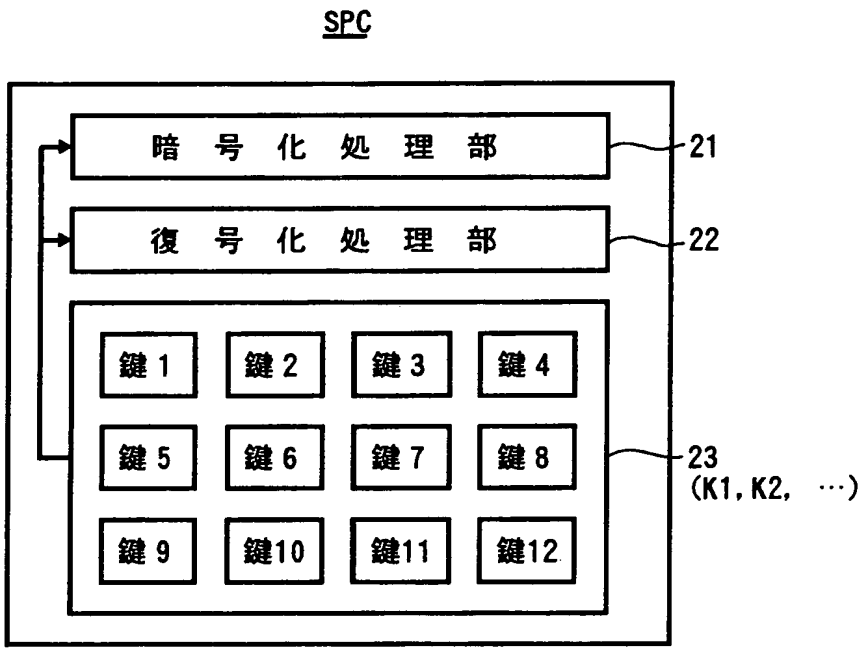
【図１】

通信システムの例を示すブロック図



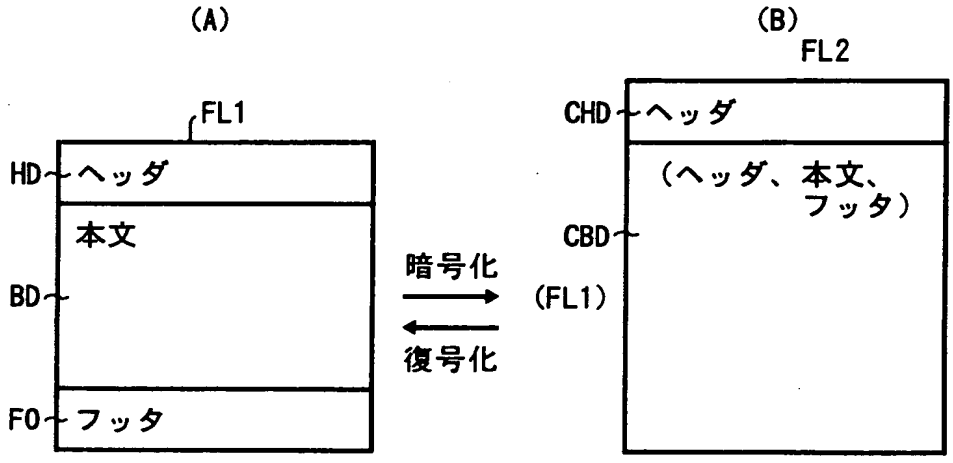
【図２】

暗号化カードの構成を示すブロック図



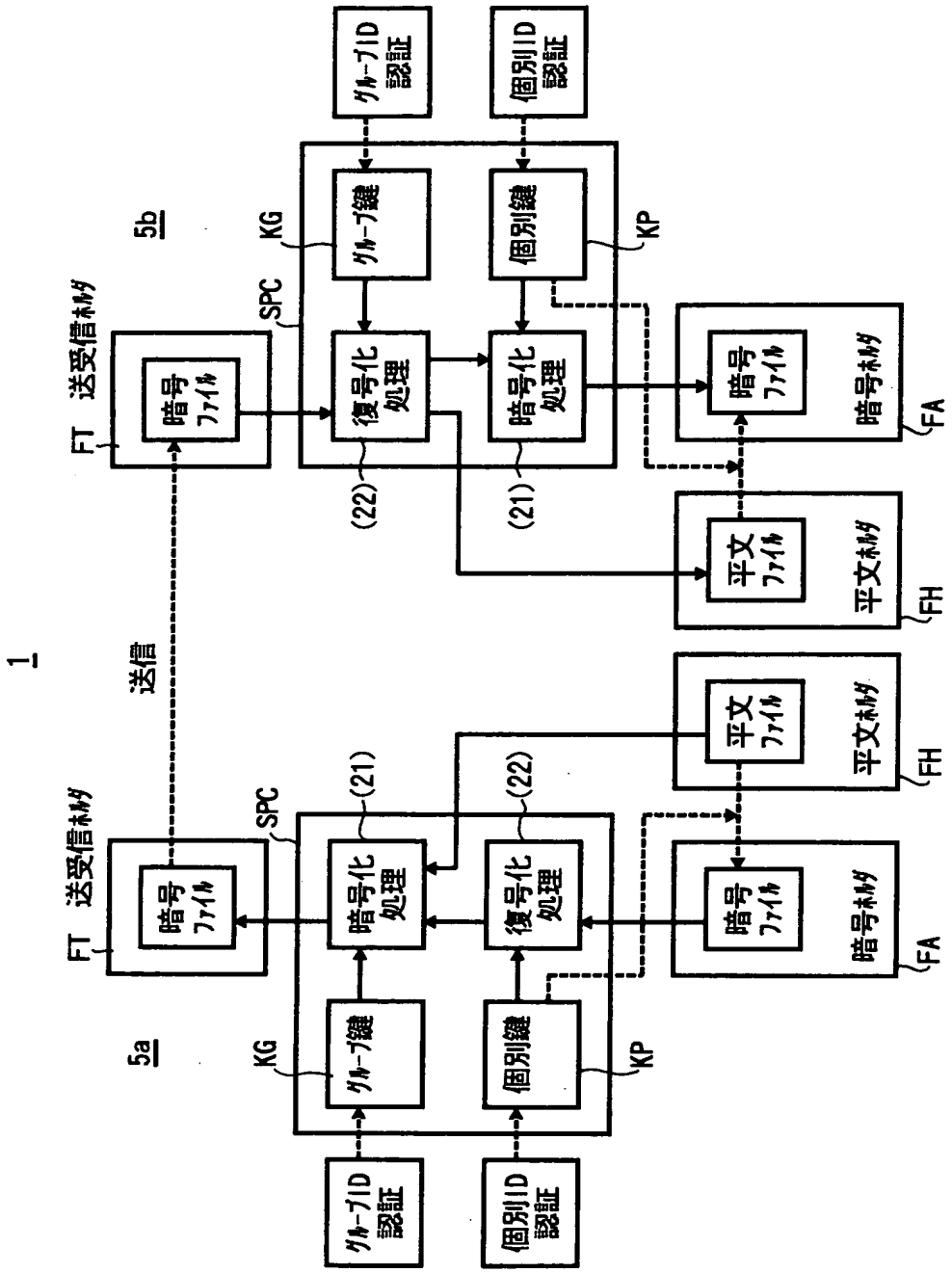
【図３】

グループ鍵により暗号化処理を行った際のファイルの状態の変化を示す図



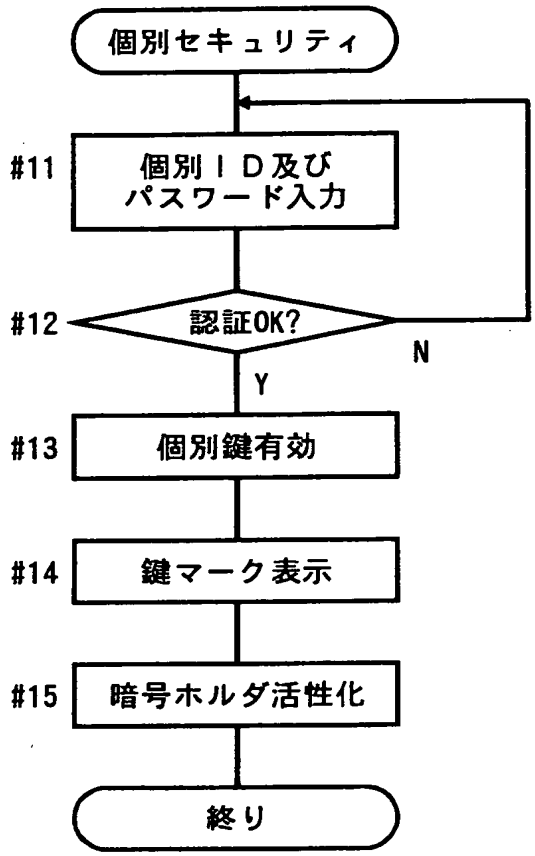
【図４】

通信端末の暗号通信時における機能を示すブロック図



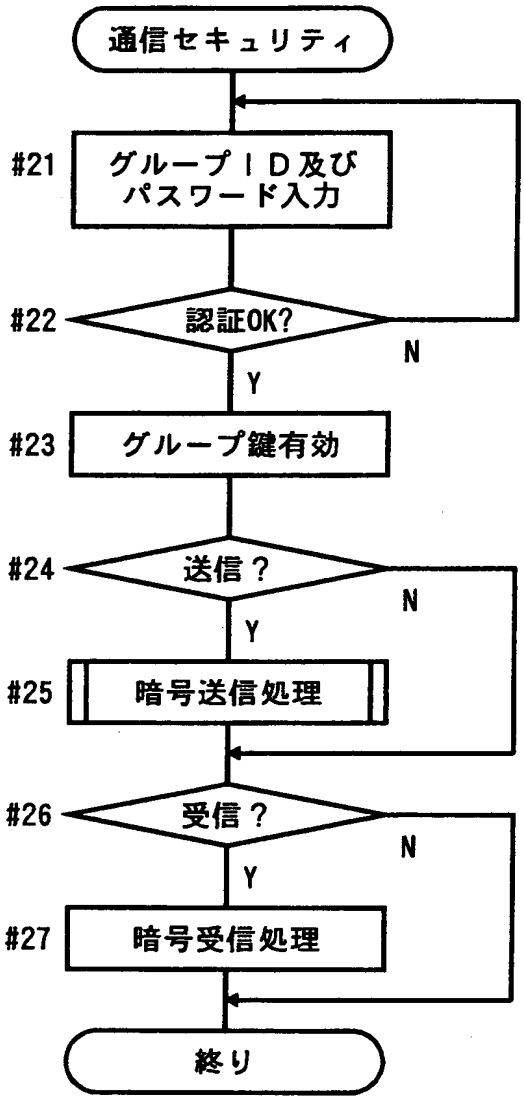
【図５】

個別セキュリティの処理を示すフローチャート



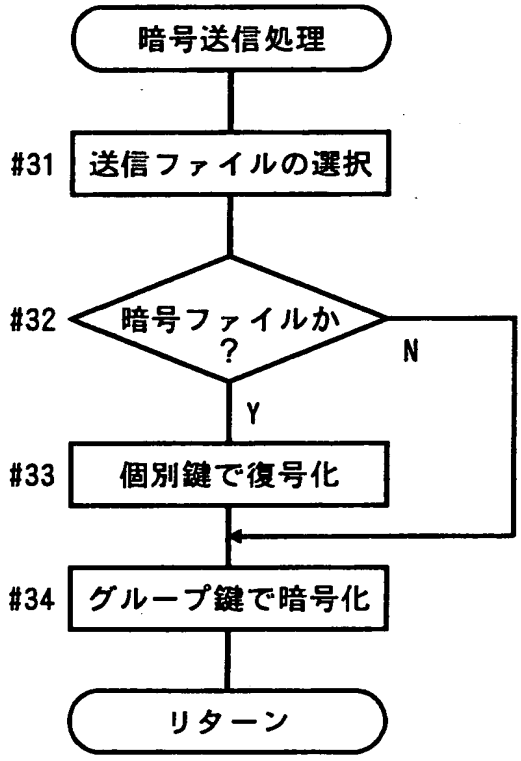
【図６】

通信セキュリティの処理を示すフローチャート



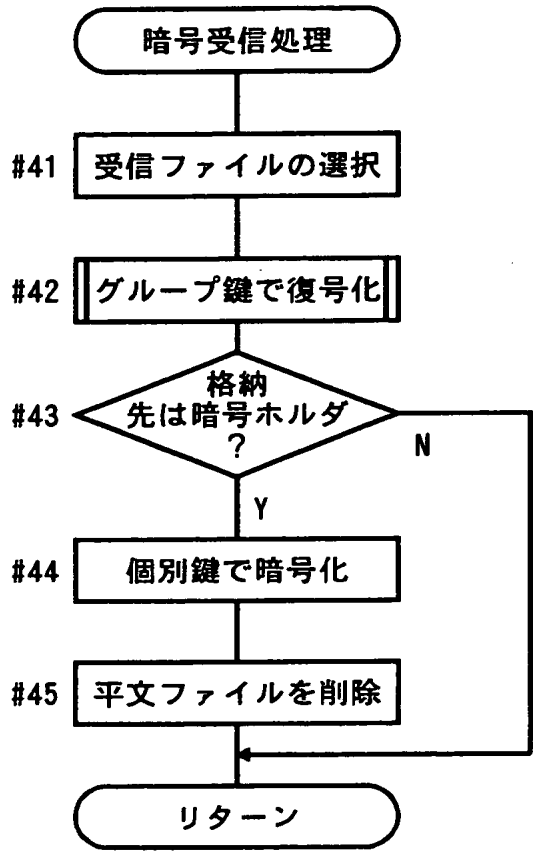
【図７】

暗号送信処理を示すフローチャート



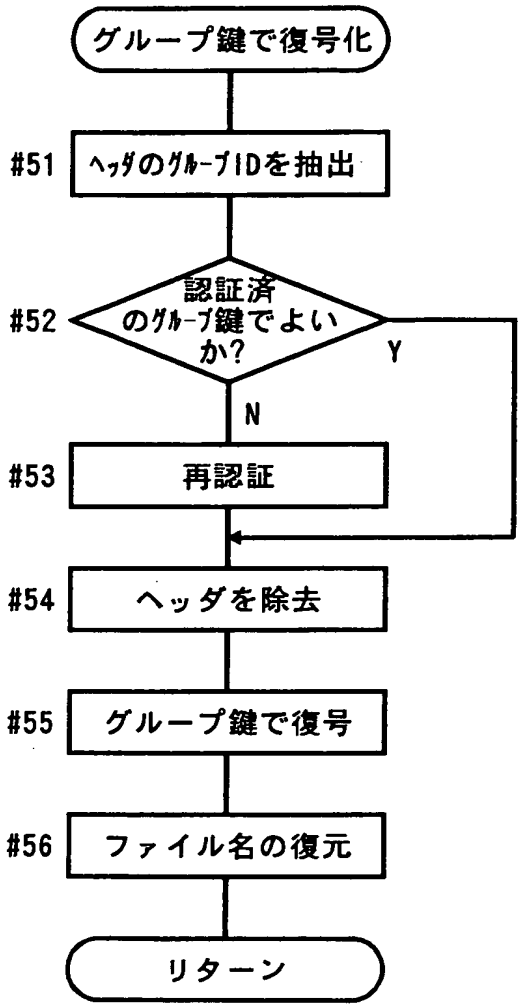
【図８】

暗号受信処理を示すフローチャート



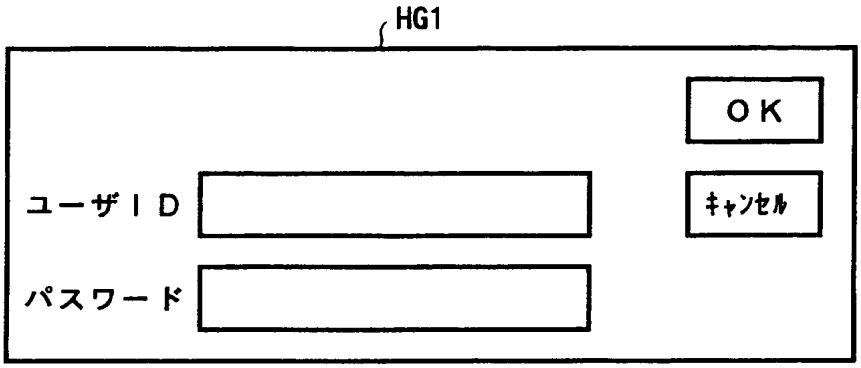
【図９】

グループ鍵での復号化処理を示すフローチャート



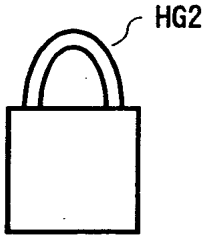
【図１０】

個別ＩＤ認証画面を示す図



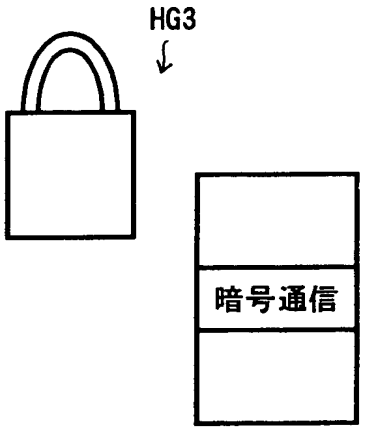
【図１１】

個別鍵が活性化された状態を示す画面



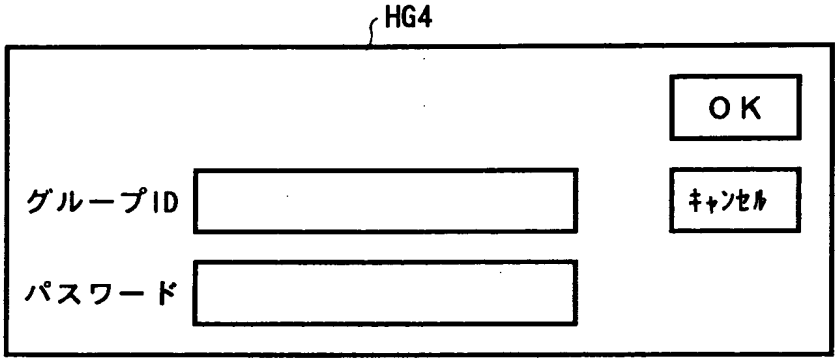
【図１２】

暗号通信のためのプルダウンメニュを示す画面



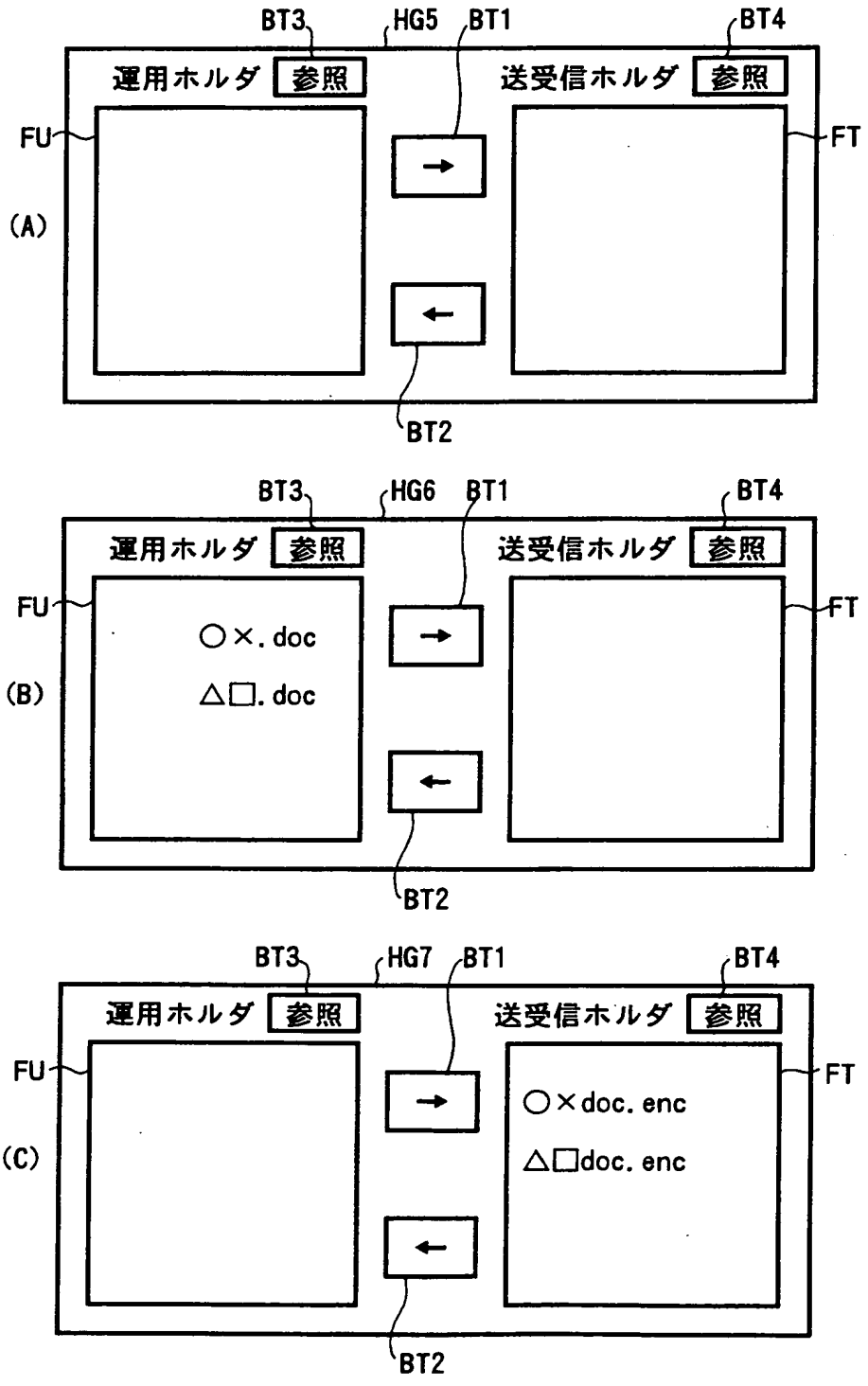
【図１３】

グループＩＤ認証画面を示す図



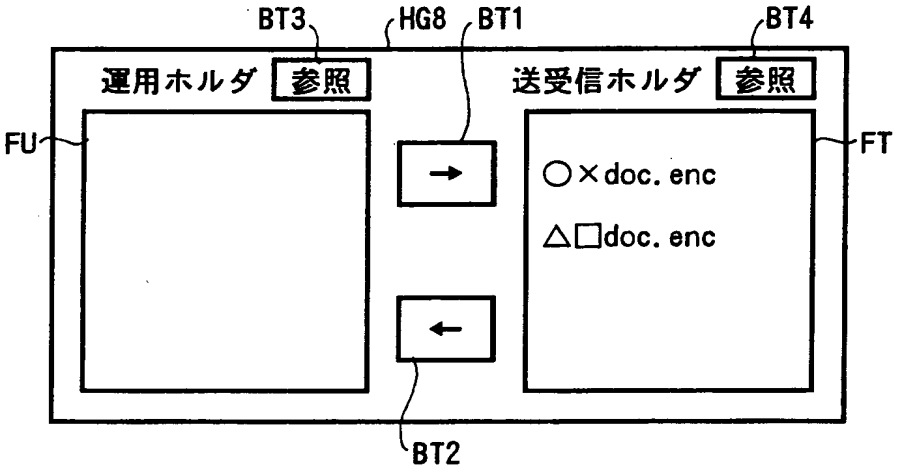
【図１４】

送信時における送信ファイルの選択の状態を示す図



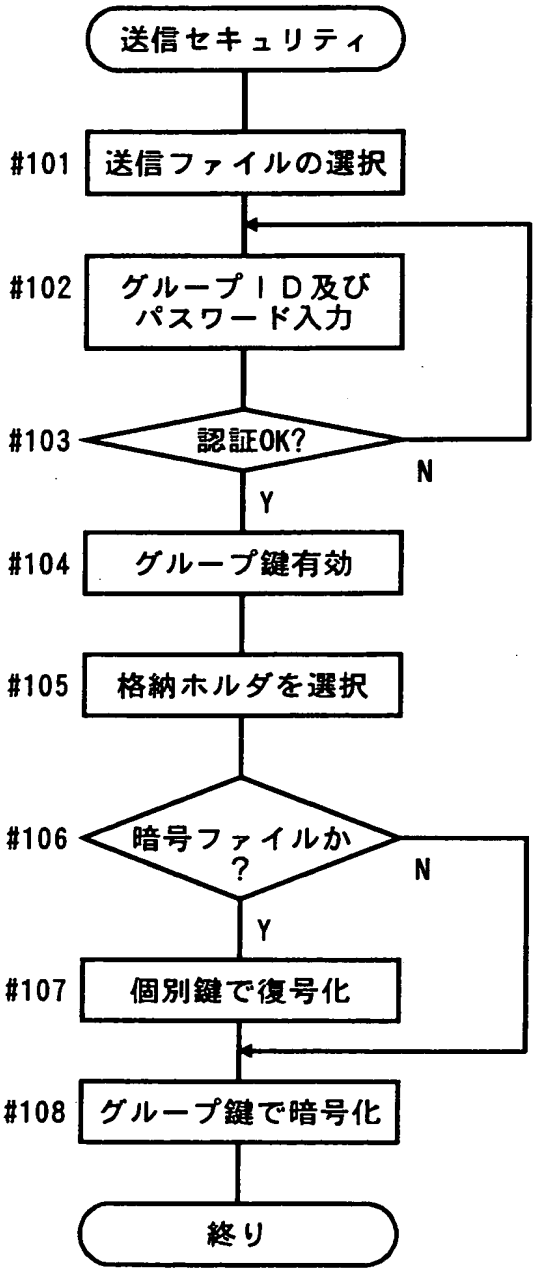
【図１５】

受信時における受信ファイルの状態を示す図



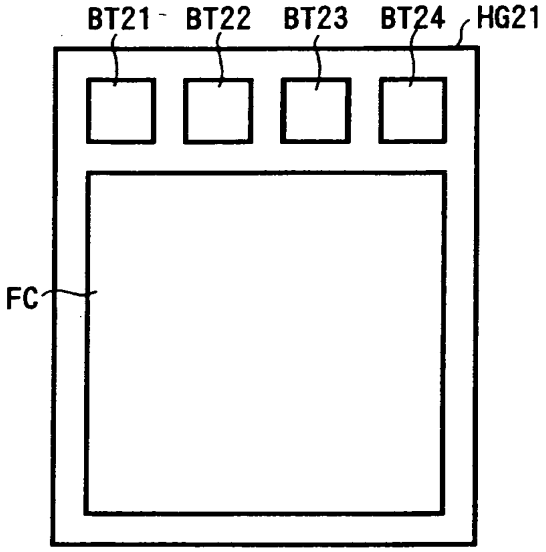
【図１６】

他の実施形態を示す送信ファイルの選択処理のフローチャート



【図１７】

ファイル選択のメイン画面を示す図



【書類名】　　要約書

【要約】

【課題】暗号化されたデータおよび暗号化されていないデータを混在して扱う場合などにおいて、容易な操作で間違うことなく暗号通信を行えるようにすること

【解決手段】送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを送信側と共通の通信用の鍵を用いて復号化する暗号通信方法であって、送信側において、通信用の鍵とは異なる個別用の鍵で暗号化されたデータを送信するに当たり、暗号化されたデータを、個別用の鍵を用いて復号化し、続いて、復号化されたデータを通信用の鍵を用いて暗号化して送信する。

【選択図】　　図７

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社